Supreme Court, U.S.
FILED
081472 MAY 29 2009
OFFICE OF THE CLERK

No.

In the Supreme Court of the United States

USA MOBILITY WIRELESS, INC.
PETITIONER,
v.
JERILYN QUON; APRIL FLORIO; JEFF QUON;
STEVE TRUJILLO,
RESPONDENTS.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

CONDITIONAL CROSS-PETITION FOR A WRIT OF CERTIORARI

J. SCOTT BALLENGER
Counsel of Record
MATTHEW A. BRILL
BARRY J. BLONIEN
LATHAM & WATKINS LLP
555 11TH STREET, NW
SUITE 1000
WASHINGTON, DC 20004
(202) 637-2200

Counsel for Cross-Petitioner

QUESTION PRESENTED

Whether the Ninth Circuit erred by holding that a service provider is liable as a matter of law under the Stored Communications Act, 18 U.S.C. §§ 2701–2712, for disclosing to a subscriber of the service the contents of communications stored in long-term archives on the provider's computers, without the consent of the sender or recipient of the message.

PARTIES TO THE PROCEEDING BELOW

Plaintiffs and appellants below were Jeff Quon, Jerilyn Quon, April Florio, and Steve Trujillo. Plaintiff Doreen Klein did not file an appeal.

Defendants and appellees below were Arch Wireless Operating Company, Inc., City of Ontario, City of Ontario Police Department, Debbie Glenn, and Lloyd Scharf.

CORPORATE DISCLOSURE STATEMENT

Arch Wireless Operating Company, Inc. ("Arch Wireless"), the original defendant in this case, has since merged into Metrocall, Inc., which later became USA Mobility Wireless, Inc. USA Mobility Wireless, Inc. is an indirect subsidiary of the publicly held USA Mobility, Inc., the nation's largest provider of paging services. No publicly held company has a 10 percent or greater ownership interest in USA Mobility, Inc., and USA Mobility, Inc. has no parent company.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

PARTIES TO THE PROCEEDING BELOW ii

CORPORATE DISCLOSURE STATEMENT ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES iv

OPINIONS BELOW 1

JURISDICTION 1

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED 1

STATEMENT OF THE CASE 2

REASONS FOR GRANTING THE WRIT 10

I. THE NINTH CIRCUIT'S READING OF THE STORED COMMUNICATIONS ACT IS INCORRECT AND UNWORKABLE 11

II. THE MEANING OF THE STORED COMMUNICATIONS ACT IMPACTS THE FOURTH AMENDMENT ANALYSIS 17

III. THE COURT SHOULD SETTLE THIS IMPORTANT ISSUE OF FEDERAL LAW 20

CONCLUSION 23

ADDENDUM

18 U.S.C. § 2510(17) 1a

18 U.S.C. § 2702(a), (b) 2a

18 U.S.C. § 2711 ..... 5a

TABLE OF AUTHORITIES

Page(s)

CASES

Ex parte Jackson,
96 U.S. 727 (1878) 14

Florida v. Riley,
488 U.S. 445 (1989) 19

Katz v. United States,
389 U.S. 347 (1967) 14, 18

Oliver v. United States,
466 U.S. 170 (1984) 18, 19

Rakas v. Illinois,
439 U.S. 128 (1978) 18, 19

SEC v. Jerry T. O'Brien, Inc.,
467 U.S. 735 (1984) 14

United States v. Councilman,
418 F.3d 67 (1st Cir. 2005) 5

United States v. Miller,
425 U.S. 435 (1976) 14

Warshak v. United States,
532 F.3d 521 (6th Cir. 2008) 3

TABLE OF AUTHORITIES—Continued

Page(s)

STATUTES

18 U.S.C. §§ 2510-2522 ..... 1, 5
18 U.S.C. § 2510(15) 4
18 U.S.C. § 2510(17) 5, 11

18 U.S.C. §§ 2701-2712 1

18 U.S.C. § 2701(a) 11

18 U.S.C. § 2702(a) 16
18 U.S.C. § 2702(a)(1) 5, 11
18 U.S.C. § 2702(a)(2) 6
18 U.S.C. § 2702(b) 6
18 U.S.C. § 2702(b)(3) 5, 6, 11

18 U.S.C. § 2703(a) 12
18 U.S.C. § 2703(b) 12, 22

18 U.S.C. § 2707 6

18 U.S.C. § 2711(2) 5, 11

28 U.S.C. § 1254(1) 1

28 U.S.C. § 1331 8

Pub. L. No. 99-508, 100 Stat. 1848 3

TABLE OF AUTHORITIES—Continued

Page(s)

LEGISLATIVE HISTORY

H.R. Rep. No. 99-647 (1986) 13, 15

S. Rep. No. 99-541 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555 ..... 4, 13, 20

OTHER AUTHORITY

Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503 (2007) 19

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) 4, 13, 16

Supreme Court Rule 12.5 1

U.S. DOJ, Computer Crime & Intellectual Prop. Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm 15

Daniel B. Yeager, *Search, Seizure, and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. Crim. L. & Criminology 249 (1993) 19

OPINIONS BELOW

The Ninth Circuit panel opinion is reported at 529 F.3d 892 (9th Cir. 2008) (Pet. App. 1–40[1]). The order denying rehearing and rehearing en banc is reported at 554 F.3d 769 (9th Cir. 2009) (Pet. App. 124–50). The opinion of the United States District Court for the Central District of California granting summary judgment in favor of Arch Wireless is reported at 445 F. Supp. 2d 1116 (C.D. Cal. 2006) (Pet. App. 41–116).

JURISDICTION

The Ninth Circuit panel issued its opinion on June 18, 2008. Arch Wireless filed a timely petition for rehearing or rehearing en banc on July 9, 2008. The Ninth Circuit issued an order denying rehearing or rehearing en banc on January 27, 2009.

The City of Ontario, the Ontario Police Department, and Lloyd Scharf (collectively, the "City Defendants") filed a petition for a writ of certiorari with this Court, which was placed on the docket on April 29, 2009 as Case No. 08-1332. USA Mobility Wireless, Inc., the successor of Arch Wireless, files this conditional cross-petition pursuant to Supreme Court Rule 12.5.

This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Relevant provisions of the Stored Communications Act, 18 U.S.C. §§ 2701–2712, and Title I of the Electronic Communications Privacy Act of 1986, 18

---

[1] "Pet. App." refers to the Appendix accompanying the Petition for a Writ of Certiorari filed by City Defendants (No. 08-1332).

U.S.C. §§ 2510–2522 are reproduced in the Addendum to this cross-petition.

STATEMENT OF THE CASE

The City of Ontario subscribed to wireless text-messaging services provided by Arch Wireless[2] and issued government-owned paging devices to members of the Ontario Police Department SWAT team for official police business. The Ninth Circuit held that the City Defendants violated the Fourth Amendment when City officials obtained from Arch Wireless archived copies of messages that SWAT team members sent and received over those devices. The Ninth Circuit also held Arch Wireless liable under § 2702 of the Stored Communications Act for releasing the message contents to the City without first securing the consent of the individual SWAT team members who sent or received those messages. The Ninth Circuit erred on both accounts.

As the City Defendants explain in their petition, the Ninth Circuit's Fourth Amendment analysis conflicts with decisions of this Court and at least seven other circuit courts by applying a "less intrusive means" test and refusing to recognize the "special needs" that are present in the context of government employment. *See* City Defs.' Pet. 21–25. More fundamentally, the Ninth Circuit's categorical determination that all users of electronic communication services have a reasonable expectation of privacy in messages stored on a service

---

[2] Arch Wireless Operating Company, Inc., the original defendant in this case, has since merged into Metrocall, Inc., which later became USA Mobility Wireless, Inc. For ease of reference, Cross-Petitioner continues to refer to "Arch Wireless" throughout this cross-petition.

provider's network disregards longstanding precedent of this Court requiring an evaluation of the particular circumstances of each case, creates a conflict with the Sixth Circuit, *see Warshak v. United States*, 532 F.3d 521, 527 (6th Cir. 2008) (en banc), and is out of step with the views of contemporary society. *See* City Defs.' Pet. 30–32.

If this Court decides to review the Fourth Amendment issues presented in the City Defendants' petition, then it should also grant this cross-petition and settle the meaning of the Stored Communications Act as applied to archived text messages. This statutory issue bears directly on the Fourth Amendment analysis and is an important issue in its own right. The Act sets two different rules for a service provider's voluntary disclosure of message contents, depending on whether the contents are (1) temporarily stored or backed up by the service provider to ensure transmission, or (2) maintained in long-term computer storage on the provider's network. The different standards reflect Congress's judgment that society does not reasonably expect that content stored indefinitely on a third party provider's servers will receive the same level of protection as content in temporary or backup storage incidental to transmission. The Ninth Circuit failed to recognize that vital distinction and, consequently, erred in holding that Arch Wireless violated the Act by disclosing archived message contents to a subscriber without the consent of the sender or recipient.

Statutory Background

Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848, "to update and clarify Federal privacy

protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. Title II of the ECPA established the Stored Communications Act, which Congress designed "to protect privacy interests in personal and propriety information, while protecting the Government's legitimate law enforcement needs." *Id.* at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557.

The Stored Communications Act focuses on the two predominant uses of computer networks at that time: "electronic communication services" and "remote computing services."[3] An "electronic communication service" includes "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Congress recognized that it is often necessary for a service provider to make a temporary copy of an electronic communication as part of the transmission process, and it sought to provide the same level of privacy protection to this incidental storage as it provided to the underlying communication itself. The Act employs "electronic storage" as a (somewhat confusing) term of art to refer only to "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B)

---

[3] As it was relatively uncommon in 1986 for individuals or even businesses to have computers capable of storing large amounts of data or performing complex data-processing tasks, many users (including banks and hospitals) would transmit their records to a third-party computing service, which would then retain the data for storage or processing. *See* S. Rep. No. 99-541, at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557; Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1213–14 (2004).

any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17). The Act distinguishes "electronic storage" from all other forms of "computer storage" (including backup functions unrelated to the delivery of a message), which are encompassed within the definition of "remote computing services." *See id.* § 2711(2) (defining "remote computing services" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

Section 2702 of the Act generally prohibits a provider of either service from voluntarily disclosing customer communications or records stored on the provider's network without consent. But the provisions governing *who* must consent to disclosure reflect Congress's judgment that disclosure of temporary copies created incident to the transmission itself raises greater privacy concerns. Indeed, some courts have held that unauthorized access of contents "in electronic storage" is functionally equivalent to interception of an electronic communication, which is prohibited under Title I of the ECPA as well as other state and federal law. *See generally* 18 U.S.C. §§ 2510–2522; *United States v. Councilman*, 418 F.3d 67, 85 (1st Cir. 2005) (en banc) (holding that interception of e-mail message "in electronic storage" violates Title I of ECPA).

Specifically, the Act states that a provider of electronic communication service "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service," 18 U.S.C. § 2702(a)(1), except "with the lawful consent of the *originator* or an addressee or *intended recipient* of such communication." *Id.* § 2702(b)(3)

(emphasis added).[4] A provider of remote computing service, which includes all other forms of computer storage and backup, *id.* § 2702(a)(2), need only obtain the consent of the "*subscriber.*" *Id.* § 2702(b)(3) (emphasis added). The statute permits any aggrieved party to recover damages for violations committed "with a knowing or intentional state of mind," and authorizes courts to award costs and attorneys fees, along with punitive damages for willful or intentional violations. *See id.* § 2707.

Factual Background[5]

Arch Wireless offers two-way text-messaging and other wireless communication services. The service generally works as follows: Arch Wireless receives a text message over its wireless network from a registered paging device and then enters that message into its computer network, where it is temporarily stored on a server.[6] Arch Wireless also makes an archived copy for long-term storage within its billing system. Arch Wireless then attempts to relay the message over its wireless network to the recipient's mobile device. The network will continue transmitting the message for up to 72 hours if the recipient is out of range or has turned off the device. Pet. App. 3. After that point, or

---

[4] The statute provides a few other limited exceptions that are not applicable here. *See* 18 U.S.C. § 2702(b).

[5] Arch Wireless limits its discussion to facts that are pertinent to the plaintiffs' Stored Communications Act claims. The City Defendants provide additional details in their petition relevant to the Fourth Amendment issues. *See* City Defs.' Pet. 3–6.

[6] The two-way text-message paging devices offer similar service to text messaging that many wireless carriers offer on wireless "smart phones," such as Blackberries.

upon delivery, the message is deleted from temporary storage. Pet. App. 3–4.

Arch Wireless maintains an archived copy of text messages in its billing system because subscribers have contacted the company in the past to inquire about messages they may have missed or to verify billing statements. ER 169.[7] The archived copies can be accessed only by employees of Arch Wireless. ER 140. According to the company's policy in place during the timeframe at issue in this lawsuit, Arch Wireless would disclose message contents only to the subscriber or a properly designated contact person for the account. ER 148–49. Arch Wireless never released contents to a user of a particular device—in fact, it often cannot determine the user's identity, because many government, healthcare, and business subscribers allow many users to share a single device. ER 153.

In 2001, Arch Wireless contracted with the City of Ontario to provide two-way text-messaging services. Pet. App. 3. The City paid a flat monthly subscription rate for each device and was allotted 25,000 characters per device per month, with overage charges for exceeding that limit. Pet. App. 6. The City was the only subscriber under the contract. ER 437.

In October 2002, the City requested that Arch Wireless provide a transcript of text messages sent to and received on certain devices for audit purposes. Pet. App. 9. Arch Wireless confirmed that the City owned the devices, verified that the person making the request was the authorized contact person, and then provided the requested transcripts. Pet. App. 8–9.

---

[7] "ER" refers to the Excerpts of Record filed with the Ninth Circuit.

Unbeknownst to Arch Wireless, Officer Jeff Quon apparently used one of the devices that the City audited. Pet. App. 54–55. The City's review of the transcripts revealed that Jeff Quon had sent sexually explicit text messages over the government-issued device to his wife, Jerilyn Quon, and to April Florio, a police dispatcher with whom he was having an affair. *Id.* Quon also sent numerous messages to Officer Steve Trujillo. Pet. App. 55.

Proceedings Below

Jeff Quon, Jerilyn Quon, April Florio, and Steve Trujillo filed a complaint in 2003 in federal district court against Arch Wireless and a number of City officials and entities. Pet. App. 10. The plaintiffs alleged, among other things, that Arch Wireless had violated § 2702 of the Stored Communications Act by releasing the contents of the text messages without obtaining Jeff Quon's consent.[8] ER 1–2.

On August 15, 2006, the district court granted summary judgment for Arch Wireless on the Stored Communications Act claim. Pet. App. 10. Based on the pleadings and record evidence, the district court found that the messages Arch Wireless archived were not in "electronic storage" because the long-term storage was not "incidental to the transmission of the communication itself, and [wa]s not meant for backup protection but apparently as the single place where text messages, after they have been read, are archived for a permanent record-keeping mechanism." Pet. App. 78. The court refused to adopt an "all or nothing" approach to characterize the services that Arch Wireless

---

[8] The plaintiffs asserted that the district court had subject matter jurisdiction pursuant to 28 U.S.C. § 1331. ER 3.

provided to the City, recognizing that while the actual provision of text messaging qualified as "electronic communication service," the storage and retrieval of archived messages constituted "remote computing services." Pet. App. 80. Therefore, the consent of the subscriber—the City—"absolve[d] Arch Wireless of liability" under § 2703(b)(3). Pet. App. 63.

The plaintiffs appealed the district court's order to the Ninth Circuit, and on June 18, 2008, the panel reversed the district court's judgment with respect to the Stored Communications Act claims and ordered that judgment be granted in the plaintiffs' favor. Pet. App. 1, 21. Even though the plaintiffs never even argued that the archived contents were in "temporary, intermediate storage . . . incidental to the electronic transmission thereof," Pet. App. 15, and they conceded at oral argument that the archived messages "were not for backup purposes"[9] within the meaning of the Act, the panel somehow concluded that "it is clear that the messages were archived for 'backup protection.'" Pet. App. 19–20. The court ruled that, "[a]s a matter of law, Arch Wireless is an 'electronic communications service' that provided text messaging service via pagers to the Ontario Police Department." Pet. App. 39. It reasoned that because the text-messaging services that Arch Wireless provided the City qualified as a "electronic communication service," *any storage* by Arch Wireless must necessarily qualify as "electronic storage" under the Act. Pet. App. 19–20. Consequently, the panel ruled that Arch Wireless violated § 2702(a)(1) when it "knowingly turned over the text-messaging transcripts

---

[9] *See* Audio Recording of Oral Argument at 5:33–5:45, *available at* http://tinyurl.com/07-55285-oa ("It is unknown why the messages are archived. They were not for backup purposes . . . .").

to the City, which was a 'subscriber,' not 'an addressee or intended recipient of such communications.'" Pet. App. 21.

Arch Wireless filed a timely petition for rehearing and rehearing en banc on July 9, 2008.[10] The Ninth Circuit issued an order denying rehearing or rehearing en banc on January 27, 2009. Pet. App. 124–25.

REASONS FOR GRANTING THE WRIT

The Fourth Amendment issues that the Ontario defendants identify in their petition are cert-worthy and important, and this Court should grant review. And if it does, it should also consider the interrelated question this cross-petition presents: whether the Stored Communications Act, properly read, prohibits a service provider from revealing to a subscriber the contents of messages that are archived in connection with the subscriber's account. That issue of statutory interpretation not only informs the "reasonable expectation of privacy" analysis that this Court would inevitably have to perform, but it independently merits the Court's attention. Unless this Court intervenes, the Ninth Circuit's erroneous construction of the Act will impact thousands of service providers (and millions of subscribers and users) within the Ninth Circuit's jurisdiction. It will also severely constrain the government's ability to obtain contents of communications in furtherance of civil and criminal investigations.

---

[10] The United States Internet Service Provider Association filed an amicus brief supporting Arch Wireless's petition. *See* Brief of Amicus Curiae United States Internet Service Provider Ass'n in Support of Petition for Rehearing and Rehearing en Banc of Appellee Arch Wireless Operating Co., *Quon v. Arch Wireless Operating Co.*, No. 07-55282 (9th Cir. July 22, 2008) (order denying reh'g and reh'g en banc) ("US ISPA Amicus Brief").

Electronic communications are ubiquitous and vital in today's society, yet the statutory and constitutional boundaries that apply to this medium remain largely unsettled. This case presents the Court an ideal opportunity to correct the Ninth Circuit's misguided understanding of the statutory framework while also resolving the Fourth Amendment issues that the City Defendants present.

I. THE NINTH CIRCUIT'S READING OF THE STORED COMMUNICATIONS ACT IS INCORRECT AND UNWORKABLE

The Stored Communications Act provides different rules to govern a service provider's voluntary disclosure of message contents in "electronic storage" as compared to other computer storage provided in connection with a "remote computing service." If a provider temporarily stores or backs up a message as part of the transmission process, *see* 18 U.S.C. § 2510(17), then the message is "in electronic storage," and the provider must obtain the sender's or recipient's consent before disclosing the contents. *See id.* § 2702(a)(1), (b)(3). All other computer storage falls within the definition of a "remote computing service," *see id.* § 2711(2), in which case the provider needs only the subscriber's consent. *See* § 2702(b)(3).

Other provisions of the Act follow the same pattern, affording less privacy protection for ordinary computer storage as compared to messages "in electronic storage" (by which the statute really means "storage incidental to transmission"). For instance, § 2701 provides criminal penalties for accessing a service provider's network without authorization and obtaining an electronic communication "while it is in electronic storage in such system." 18 U.S.C. § 2701(a). There is

no similar criminal provision addressing unauthorized access of content stored in connection with "remote computing services." Section 2703 requires the government to obtain a search warrant to compel disclosure of contents in "electronic storage" for less than 180 days, whereas the government may use an administrative subpoena or court order to obtain contents stored in connection with a "remote computing service" or contents "in electronic storage" for longer than 180 days. 18 U.S.C. § 2703(a), (b).[11]

The Ninth Circuit recognized that different rules applied to providers of "remote computing services" and providers of "electronic communication services," *see* Pet. App. 14, but it incorrectly assumed that a provider may have only one classification for all of the services it provides, at all times. The court mistakenly reasoned that because Arch Wireless provided the underlying transmission of the text messages, it must be an "electronic communication service" for all purposes, and any storage provided by Arch Wireless must be "electronic storage," regardless of whether the storage was incidental to transmission. Pet. App. 16.

The Ninth Circuit's holding is impossible to square with the statutory text. As the terms "electronic communication *service*" and "remote computing *service*" themselves make clear, these concepts apply to specific services, not to any blanket characterization of the *provider*. The specific context is critical in determining

---

[11] It might seem odd that a message could remain in "temporary" storage for such a long period, but that scenario could easily arise. For instance, an e-mail user might check an account infrequently, in which case any pending messages would remain "in electronic storage" on the service provider's network until the recipient actually retrieves those messages.

the statutory classification. An entity may provide "electronic communication services" in some contexts and "remote computing services" in others, even with respect to the same message—the proper classification entirely depends on the purpose of storage at a specific point in time. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1215 (2004) (observing that "most network service providers are multifunctional," and the statutory classification is "context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract"). A provider of electronic communication services retains that classification only to the extent it temporarily copies or backs up a message in order to facilitate transmission; all other storage services it provides are classified as "remote computing services."

The legislative history confirms that a provider of remote computing services "may also provide electronic communication services," S. Rep. No. 99-541, at 14, *as reprinted in* 1986 U.S.C.C.A.N. at 3568, and that different aspects of the same communication may be entitled to different treatment under the Act. A House Report accompanying the bill observed, for instance, that "[s]ometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time." H.R. Rep. No. 99-647, at 65 (1986). Such communication, the Report explained, "should continue to be covered by section 2702(a)(2)"—the provision addressing remote computing services. *Id.*

Congress's apparent belief that information temporarily stored incident to transmission itself is more private or sensitive than long-term archives may have

been inspired by (or an effort to accommodate) the Fourth Amendment principles as articulated by this Court. Specifically, this Court has long recognized that a party maintains no expectation of privacy over information voluntarily provided to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984). At the same time, however, this Court has repeatedly held that the government may not eavesdrop on a phone call or open a sealed package in the mail—even though those methods of communication similarly involve providing information to a third party. *See, e.g., Katz v. United States*, 389 U.S. 347, 352 (1967); *Ex parte Jackson*, 96 U.S. 727, 733 (1878). Congress likely made the judgment that a service provider should be treated as a carrier (much like the post office or telephone company) when it provides an electronic communication service and stores contents incident to the transmission of the message, but that a provider is more like a traditional third party when it simply maintains contents in long-term storage.

The distinction between "electronic storage" and other "computer storage" may be somewhat confusing, particularly because long-term storage archives are often referred to as "backup" copies in the everyday use of that term. In the context of the Act, however, it is clear that Congress intended the phrase "for purposes of backup protection of such communication" to be construed more narrowly to encompass only backup copies made to ensure transmission of the message. A broader reading of "backup" makes no sense in the overall structure of the statute, because all

"computer storage" maintained by the provider of electronic communication services would then qualify as "electronic storage" within the meaning of § 2510(17), effectively collapsing the two categories of services and eliminating the less stringent standards that apply to "remote computing services." The legislative history validates the narrower construction. The House Report explained that the purpose of "[b]ackup protection" is to "preserve[] the integrity of the electronic communications system and to some extent preserve[] the property of the users of such a system," and to the extent a message is stored longer than necessary to ensure transmission, "it is closer to a regular business record maintained by a third party, and, therefore, deserving of a different standard of protection." H.R. Rep. No. 99-647, at 68.

DOJ has adopted the view that "electronic storage" refers only to storage that is incidental or related to transmission of the communication. For example, in a DOJ manual addressing the search and seizure of computers and stored communications, DOJ states that an e-mail stored on a network after the recipient has retrieved and viewed the message "is no longer in 'electronic storage'" but is "simply a remotely stored file," because "the process of transmission to the intended recipient has been completed."[12] And in an amicus brief filed in another Ninth Circuit case, DOJ argued that reading 'electronic storage' too broadly "effectively obliterates the [Act's] essential distinction" between "electronic storage" and other computer

---

[12] U.S. DOJ, Computer Crime & Intellectual Prop. Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* § II.B (2002), *available at* http:// www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm.

storage maintained in connection with "remote computing service."[13] Professor Orin Kerr agrees: He explained that the "traditional understanding has been that a copy of [an] opened e-mail sitting on a server is protected" only by the remote computing service rules because "that copy is no longer 'incident to transmission' nor a backup copy of a file that is incident to transmission; rather, it is just in remote storage like any other file held by" a provider of remote computing service. Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. at 1216.

Arch Wireless unquestionably acts as an "electronic communication service" provider when it transmits text messages over its network, and its temporary storage of contents in connection with the transmission process constitutes "electronic storage." But that aspect of its services is not at issue. The plaintiffs allege that Arch Wireless violated the Stored Communications Act by divulging to the City the contents of messages that were retrieved from its long-term archives—long after the messages were delivered and the temporary storage was deleted. The sole question is whether the archived messages stored in its billing system were "in electronic storage" when they were disclosed. *See* 18 U.S.C. § 2702(a). The plaintiffs have never argued that this storage was "incidental to the electronic transmission," and they conceded at oral argument that the storage was not for backup

---

[13] Brief for the United States as Amicus Curiae Supporting Defendant/Appellee's Petition for Rehearing and Suggestion for Rehearing en Banc at 11, *Theofel v. Farey Jones*, No. 02-15742 (9th Cir. Sept. 25, 2003).

purposes.[14] That concession is plainly correct. Individual users had no access to content archived in long-term storage, and even if they had access, the archived messages could not have been used to retransmit the original communication because they were stored in a completely different form than the original message. Arch Wireless maintained a copy of the text message contents for purposes completely unrelated to the transmission of the original message; specifically, Arch Wireless periodically responded to subscribers' questions about billing statements or missed messages. ER 169.

Because there is no legitimate dispute that the archived messages were no longer "in electronic storage" when Arch Wireless provided them to the City, the company cannot be liable under the Act. The Ninth Circuit's holding that, "[a]s a matter of law, Arch Wireless is an 'electronic communication service'" makes no sense, disregards the undisputed facts, and is a plain misreading of the statute. Pet. App. 39.

II. THE MEANING OF THE STORED COMMUNICATIONS ACT IMPACTS THE FOURTH AMENDMENT ANALYSIS

This Court should review the Ninth Circuit's erroneous construction of the Stored Communications Act alongside the Fourth Amendment issues that the City Defendants present in their petition. Review of this statutory issue would not require any additional analysis beyond the Fourth Amendment issues, and this case presents an ideal opportunity for the Court to

---

[14] *See* Audio Recording of Oral Argument at 5:33–5:45, *available at* http://tinyurl.com/07-55285-oa ("It is unknown why the messages are archived. They were not for backup purposes . . . .").

correct the Ninth Circuit's misguided understanding of the statutory framework. This Court invariably will confront the meaning of the Stored Communications Act in determining whether the plaintiffs actually have a "reasonable expectation of privacy" in the contents of text messages stored on a third party's servers, as they have alleged. The Ninth Circuit's analysis altogether disregards the considered judgment of Congress that messages in long-term storage deserve less privacy protection than messages that are stored or backed up temporarily in connection with the transmission process, and that error likely clouded the Ninth Circuit's Fourth Amendment analysis.

Modern Fourth Amendment analysis usually begins with *Katz v. United States*, in which Justice Harlan first articulated the "reasonable expectation of privacy" test. *See* 389 U.S. at 360 (Harlan, J., concurring). He wrote that, in order for the Fourth Amendment to protect an individual from an unwanted government intrusion, the person must first demonstrate "an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361. This Court has conducted a searching inquiry into all relevant factors, including "the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government intrusion." *Oliver v. United States*, 466 U.S. 170, 178 (1984) (citations omitted).

Although no single factor resolves whether an expectation of privacy is reasonable in all cases, the rights afforded by positive law are and always have been an important factor in the calculus. In *Rakas v.*

Illinois, for instance, the Court observed that even after *Katz*, the "[l]egitimation of expectations of privacy by law must have a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." 439 U.S. 128, 143 n.12 (1978).[15] In *Oliver v. United States*, the Court recognized that the existence of a property right remains an "element in determining whether expectations of privacy are legitimate," although that fact alone is not always sufficient to establish a legitimate expectation of privacy (and was not sufficient in that case). *Oliver*, 466 U.S. at 183.[16] And in *Florida v. Riley*, the plurality determined that helicopter surveillance at low altitude did not violate the Fourth Amendment, in part because "the helicopter in this case was *not* violating the law." 488 U.S. 445, 451 (1989).[17]

In conducting the thorough analysis that *Katz* demands, this Court will take into account the lines that Congress has already drawn that clearly impact

---

[15] *See also* 439 U.S. at 153 (Powell, J., concurring) ("[A]s the Court states today, property rights reflect society's explicit recognition of a person's authority to act as he wishes in certain areas, and therefore should be considered in determining whether an individual's expectations of privacy are reasonable.").

[16] *See also* 466 U.S. at 189 (Marshall, J., dissenting) ("As the Court acknowledges, we have traditionally looked to a variety of factors in determining whether an expectation of privacy . . . is 'reasonable,'" including "whether the expectation at issue is rooted in entitlements defined by positive law.").

[17] For additional cases and a more extensive discussion of the Court's use of positive law in Fourth Amendment analysis, *see generally* Daniel B. Yeager, *Search, Seizure, and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. Crim. L. & Criminology 249 (1993); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503 (2007).

the Fourth Amendment issues presented in this case. The Stored Communications Act reflects Congress's judgment concerning the extent to which electronic messages archived in long-term storage on a provider's network should be protected from disclosure. *See* S. Rep. No. 99-541, at 5, *as reprinted in* 1986 U.S.C.C.A.N. at 3559 ("The Committee believes that [the ECPA] represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."). This Court might ultimately conclude that this statutory framework does not, by itself, provide a sufficient basis to resolve the Fourth Amendment issue, but it clearly informs the analysis.

The statutory issues presented in this cross-petition will not require additional analysis beyond the constitutional analysis, and, as explained below, the Ninth Circuit's erroneous construction of the statute has significant, far-reaching consequences aside from its bearing on the Fourth Amendment analysis. Thus, if the Court decides to resolve the Fourth Amendment issues the City Defendants present, the Court should also settle the meaning of the statute as applied to the facts of this case.

III. THE COURT SHOULD SETTLE THIS IMPORTANT ISSUE OF FEDERAL LAW

The impact of the Ninth Circuit's ruling is not limited to the parties in this case, or even to other providers of two-way text messaging services. It affects all electronic communication service providers, including Internet service providers, wireless phone companies, and many others. Many of the world's leading providers of computing and online services are located within the Ninth Circuit. They and their

customers are all directly affected by this decision. The Ninth Circuit's ruling will have a host of unintended consequences if it remains the law, while generating no significant benefit to privacy interests.

Under the Ninth Circuit's analysis, any storage maintained by a provider of electronic communications constitutes "electronic storage," and providers must therefore secure the consent of senders and recipients before they can reveal such content to the subscriber of the service. For many providers that retain messages in long-term storage, including Arch Wireless, it likely would be impossible to implement a disclosure policy that complies with the Ninth Circuit's decision.

As the United States Internet Service Provider Association ("US ISPA") explained in its amicus brief in support of rehearing and rehearing en banc, many services allow families and businesses to share a single account.[18] In addition, hospitals, police departments, and other commercial and government employers often assign a wireless device to whomever is working a particular shift, rather than dedicating the device for an individual employee's exclusive use. Accordingly, it is impossible in many cases for the provider to ascertain who sent a particular message. Yet subscribers normally expect to have control and access over all aspects of their account, including access to any e-mails and other messages sent by other users. The Ninth Circuit's ruling would significantly frustrate that expectation. As the US ISPA observed, the Ninth Circuit's decision would cause subscribers to "lose significant control over how the service is being used, especially in connection with the stored communi-

---

[18] *See* US ISPA Amicus Brief at 6.

cations of shared or sub-account holders or other informal users" of the service.[19]

The Ninth Circuit's decision also undermines an employer's ability to rely on an official policy stating that employees have no privacy interest in e-mails and text messages sent using company-provided devices. If the unofficial actions of a single supervisor can negate that policy—and thereby subject the service provider to significant liability risks—then many providers will conclude that the subscriber's consent is no longer adequate to warrant disclosure. As a result, Arch Wireless and other providers may be forced to stop archiving messages altogether, even though many subscribers demand such features to verify aspects of their bills and for other legitimate reasons. Even where a service provider could identify the particular sender or recipient of a message, the Ninth Circuit's ruling will impose considerable administrative costs and would force providers into a potentially adversarial relationship with their subscribers.

The Ninth Circuit's overbroad construction of "electronic storage" also casts confusion over the compulsory disclosure provisions of the Stored Communications Act and upsets the careful balance that Congress struck between privacy interests and law enforcement needs. The Act expressly authorizes law enforcement to obtain contents in long-term storage with an administrative subpoena, *see* 18 U.S.C. § 2703(b), but the Ninth Circuit's construction would require law enforcement to obtain a warrant before accessing any such information, severely limiting their ability to carry out civil and criminal investigations.

---

[19] US ISPA Amicus Brief at 6.

For instance, the Government would have a far more difficult time accessing e-mails and text messages stored on providers' servers, even long after those messages have been received and read. And of course if service providers altogether stop archiving electronic messages as a consequence of the Ninth Circuit's ruling, then law enforcement will be unable to access such information under any circumstances—even with a warrant. Quite plainly, electronic communications are critically important in today's society, and the Ninth Circuit's ruling will deal a significant blow to law enforcement efforts.

CONCLUSION

For the reasons set forth above, if this Court grants review of the Fourth Amendment issues presented in the City Defendants' petition, then it should also grant this cross-petition and review the question USA Mobility Wireless, Inc. presents.

Respectfully submitted,

J. SCOTT BALLENGER
Counsel of Record
MATTHEW A. BRILL
BARRY J. BLONIEN
LATHAM & WATKINS LLP
555 11TH STREET, NW
SUITE 1000
WASHINGTON, DC 20004
(202) 637-2200

Counsel for Cross-Petitioner

ADDENDUM

TABLE OF CONTENTS TO ADDENDUM

18 U.S.C. § 2510(17) 1a

18 U.S.C. § 2702(a), (b) 2a

18 U.S.C. § 2711 ..... 5a

18 U.S.C. § 2510 (17)

§ 2510. Definitions

As used in this chapter—

* * *

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

* * *

18 U.S.C. § 2702

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such

service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108-21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

* * *

18 U.S.C. § 2711

§ 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.